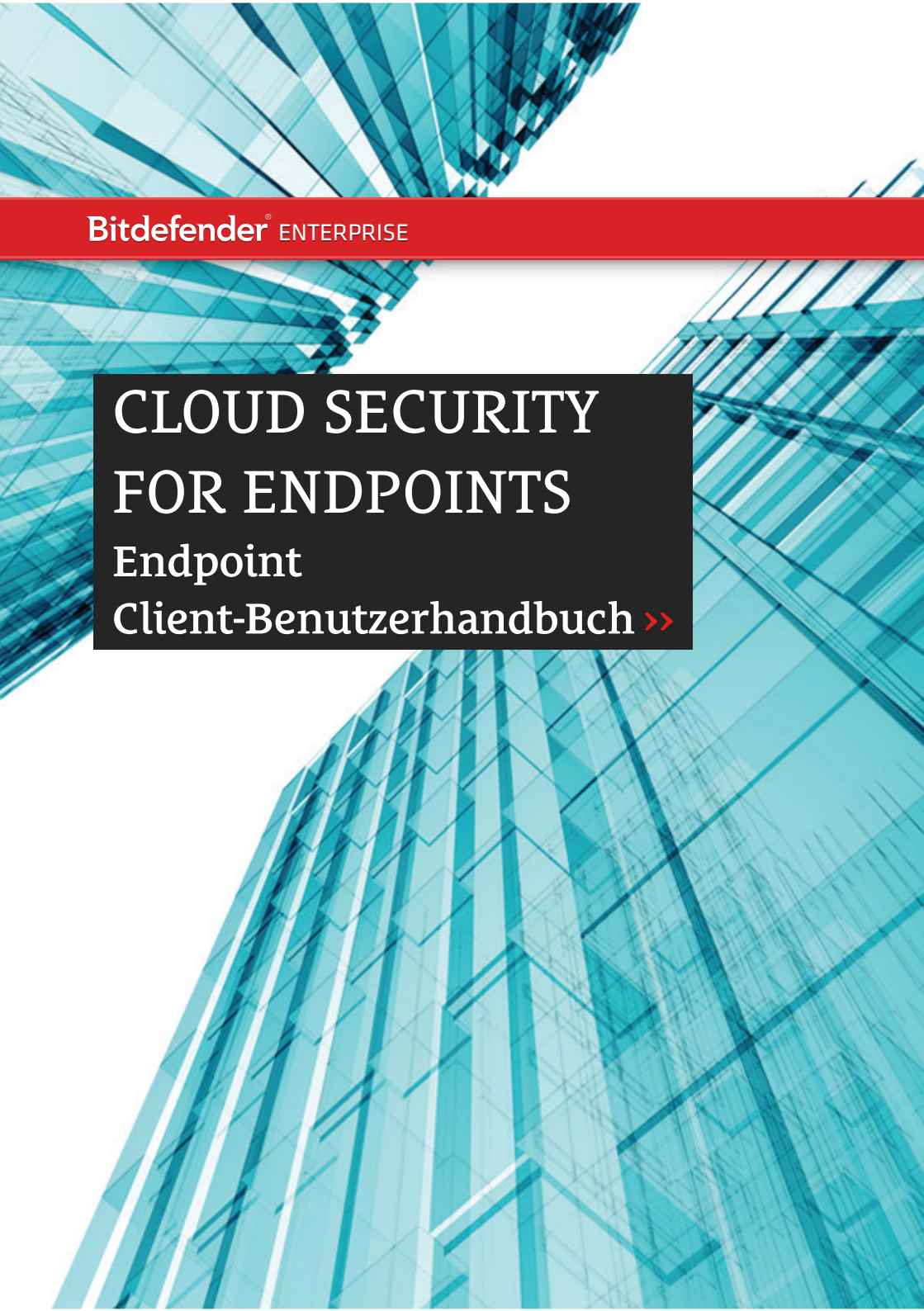

Bitdefender ENTERPRISE
CLOUD SECURITY
FOR ENDPOINTS
Endpoint
Client-Benutzerhandbuch ››

Cloud Security for Endpoints by Bitdefender
Endpoint Client-Benutzerhandbuch

Veröffentlicht 2012.11.16

Copyright© 2012 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Company. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation ist urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „wie besehen" zur Verfügung gestellt und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokumente entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere Webseiten, die nicht von Bitdefender erstellt wurden, und auch nicht von ihr kontrolliert werden können. Somit übernimmt Bitdefender auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. Bitdefender stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass Bitdefender in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Bitdefender

Inhaltsverzeichnis

Zur Verwendung dieses Handbuchs v
1. Zielsetzung und Zielgruppe v
2. Über dieses Handbuch v
3. Konventionen in diesem Handbuch v
4. Ihre Mithilfe vi

1. Erste Schritte 1
1.1. System Tray Icon 1
1.2. Öffnen des Hauptfensters 2
1.3. Hauptfenster 2
1.3.1. Obere Symbolleiste 3
1.3.2. Tafelbereich 4
1.4. Surf-Schutz 6
1.4.1. Bitdefender-Symbolleiste 7
1.4.2. Suchberater 7
1.4.3. Gesperrte Webseiten 7
1.5. Geräte-Scan 8
1.6. Anpassen von Schutzeinstellungen 8

2. Prüfung auf Malware 9
2.1. Scannen von Dateien und Ordnern 9
2.2. Ausführen eines Quick Scans 9
2.3. Ausführen eines vollständigen System-Scans 10
2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans 10
2.5. Antivirus Prüfassistent 14
2.5.1. Schritt 1 - Führen Sie den Scan durch 14
2.5.2. Schritt 2 - Wählen Sie entsprechende Aktionen aus 15
2.5.3. Schritt 3 - Zusammenfassung 16
2.6. Scan-Protokolle werden überprüft 16

3. Updates 18
3.1. Arten von Updates 18
3.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist 19
3.3. Durchführung eines Updates 19
3.4. Wobei handelt es sich bei der Frequenz für automatische Updates? 20

4. Ereignisse 21

5. Hilfe erhalten 22

Glossar 23

Zur Verwendung dieses Handbuchs

1. Zielsetzung und Zielgruppe

Diese Dokumentation richtet sich an die Endanwender von **Endpoint Client**, der Cloud Security for Endpoints-Client-Software, die auf Computern und Servern installiert wird, um diese vor Malware und anderen Bedrohungen aus dem Internet zu schützen und die Einhaltung von Richtlinien für die Benutzerkontrolle sicherzustellen.

Die hier bereitgestellten Informationen sollten für jeden Benutzer mit Erfahrung im Umgang mit Windows verständlich sein.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

2. Über dieses Handbuch

Dieses Handbuch ist übersichtlich gestaltet, damit Sie im Handumdrehen alle benötigten Informationen finden können.

„Erste Schritte“ (S. 1)
Machen Sie sich mit der Endpoint Client-Benutzeroberfläche vertraut.

„Prüfung auf Malware“ (S. 9)
Erfahren Sie, wie Sie Malware-Scans ausführen können.

„Updates“ (S. 18)
Erfahren Sie mehr über Endpoint Client-Updates.

„Ereignisse“ (S. 21)
Überprüfen Sie die Aktivität von Endpoint Client.

„Hilfe erhalten“ (S. 22)
Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

3. Konventionen in diesem Handbuch

Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der unten stehenden Tabelle entnehmen.

Erscheinungsbild	Beschreibung
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Zur Verwendung dieses Handbuchs“ (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`Dateiname`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch **Fettdruck** hervorgehoben.

Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.

Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

4. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse documentation@bitdefender.com kontaktieren.Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

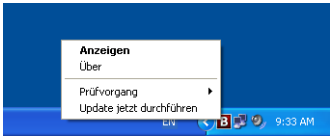
1. Erste Schritte

Endpoint Client ist eine vollständig automatisiertes Computer-Sicherheitslösung, die per Fernzugriff von Ihrem Netzwerkadministrator oder Dienstleister verwaltet wird. Nach der Installation schützt sie Sie vor allen Arten von Schad-Software (wie Viren, Spyware und Trojaner), Netzwerkangriffen, Phishing-Versuchen und Datendiebstahl. Zudem kann sie genutzt werden, um die Einhaltung von Unternehmensrichtlinien zur Computer- und Internet-Nutzung sicherzustellen.

Endpoint Client trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen.Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Ereignisfenster.Für weitere Informationen lesen Sie bitte „Ereignisse“ (S. 21).

1.1. System Tray Icon

Nach der Installation wird ein Endpoint Client-Symbol dauerhaft in Ihrer Task-Leiste angezeigtEin Doppelklick auf dieses Symbol öffnet das Hauptfenster des Programms. Mit einem Rechtsklick auf das Symbol öffnen Sie ein Kontextmenü mit nützlichen Optionen.



System Tray Icon

- **Anzeigen** - Öffnet das Endpoint Client-Hauptfenster.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Endpoint Client erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.
- **Scan** - Hiermit können Sie Malware-Scans durchführen.Sie können zwischen drei Scan-Aufgaben auswählen:
  - Beim **Quick Scan** wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.
  - **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.
  - Der **vollständige System-Scan** durchsucht den gesamten Computer nach allen Typen von Schad-Software, die ein Sicherheitsrisiko darstellen, so z.B. Viren, Spyware, Adware, Rootkits usw.

  Weitere Informationen zur Nutzung der Scan-Aufgaben finden Sie unter „Prüfung auf Malware“ (S. 9).

- **Jetzt Aktualisieren** - startet ein sofortiges Update.Sie können den Update-Status in dem eingeblendeten Fenster verfolgen.

Das Bitdefender-Symbol in der Task-Leiste weist Sie durch die folgenden Farbwechsel auf Probleme hin, die Ihren Computer beeinträchtigen:

Kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.

Nicht-kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.

Wenn Endpoint Client nicht aktiv ist, ist das Symbol in der Task-Leiste grau hinterlegt: .Dies geschieht in der Regel dann, wenn der Lizenzschlüssel abgelaufen ist. Es ist auch möglich, dass die Bitdefender-Dienste nicht antworten oder andere Fehler die normale Ausführung des Programms behindern.

Beachten Sie
Sollte das Problem weiterhin bestehen, wenden Sie sich bitte an Ihren Netzwerkadministrator oder Dienstleister.

1.2. Öffnen des Hauptfensters

Sie können die Benutzeroberfläche von Endpoint Client aus dem Windows-Startmenü heraus über den folgenden Pfad aufrufen: **Start** → **Alle Programme** → **Endpoint Client** → **Endpoint Client**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol in der Task-Leiste.

1.3. Hauptfenster

Im Endpoint Client-Hauptfenster können Sie den Schutzstatus überprüfen und grundlegende Sicherheitsaufgaben ausführen (Updates und Scans).Und das alles mit nur wenigen Klicks.Die Konfiguration und Verwaltung des Schutzes erfolgt per Fernzugriff durch Ihren Netzwerkadministrator oder Dienstleister.

Hauptfenster

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

Obere Symbolleiste
: Hier können Sie den Sicherheitsstatus Ihres Computers überprüfen und auf wichtige Aufgaben zugreifen.

Tafelbereich
: Hier können Sie den Status der verschiedenen Schutzmodule überprüfen.

Zusätzlich finden Sie eine Reihe nützlicher Support-Optionen im unteren Bereich des Fensters:

Optionen	Beschreibung
Online-Hilfe	Klicken Sie auf diesen Link, wenn Sie Hilfe zu Endpoint Client benötigen.
	Klicken Sie auf dieses Symbol, um Produkt- und Kontaktinformationen anzuzeigen.

1.3.1. Obere Symbolleiste

Die obere Symbolleiste enthält die folgenden Elemente:

- Der **Sicherheitsstatusbereich** auf der linken Seite der Symbolleiste informiert Sie über Probleme, die die Sicherheit Ihres Computers beeinträchtigen.Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

- **Der Bereich ist grün markiert.**Es müssen keine Probleme behoben werden.Ihr Rechner und Ihre Daten sind geschützt.
- **Der Bereich ist gelb markiert.**Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt.
- **Der Bereich ist rot markiert.**Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Sie können die erkannten Sicherheitsprobleme anzeigen, indem Sie auf eine beliebige Stelle im Sicherheitsstatusbereich klicken.Bestehende Probleme werden von Ihrem Netzwerkadministrator behoben.

- **Ereignisse** Hier können Sie eine detaillierte Übersicht aller relevanten Ereignisse abrufen, die aufgetreten sind, während das Produkt aktiv war.Für weitere Informationen lesen Sie bitte „Ereignisse“ (S. 21).
- **Update** öffnet das Update-Status-Fenster und lässt Sie ein Update anfordern.Für weitere Informationen lesen Sie bitte „Updates“ (S. 18).

1.3.2. Tafelbereich

Im Tafelbereich können Sie den Status der Schutzmodule überprüfen.Es gibt einen eigenständigen Bereich für jedes Schutzmodul.

Der Schutzstatus wird in der oberen rechten Ecke des Fensters mithilfe der folgenden Symbole angezeigt:

ON Schutz ist aktiviert.
OFF Schutz ist deaktiviert.

Wenn ein Schutzmodul nicht installiert ist, wird eine entsprechende Nachricht über dem betroffenen Bereich angezeigt.

In diesem Bereich stehen Ihnen die folgenden Tafeln zur Verfügung:

Malware-Schutz

Der Malware-Schutz bildet die Grundlage Ihrer Sicherheit. Endpoint Client schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Malware, so zum Beispiel vor Viren, Trojanern, Spyware, Adware usw.

Im Bereich Malware-Schutz können Sie schnell und einfach auf wichtige Scan-Aufgaben zugreifen.Klicken Sie auf **Jetzt scannen** und wählen Sie dann eine Aufgabe aus dem Dropdown-Menü:

- Beim **Quick Scan** wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

- **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.
- Der **vollständige System-Scan** durchsucht den gesamten Computer nach allen Typen von Schad-Software, die ein Sicherheitsrisiko darstellen, so z.B. Viren, Spyware, Adware, Rootkits usw.

Weitere Informationen zur Nutzung der Scan-Aufgaben finden Sie unter „Prüfung auf Malware“ (S. 9).

Firewall

Die Firewall schützt Sie, wenn Sie mit Netzwerken und dem Internet verbunden sind, indem sie Verbindungsversuche filtert und verdächtigte oder gefährliche Verbindungen blockiert.

Details zu Ihrer Firewall-Konfiguration erhalten Sie über einen Klick auf die Schaltfläche **Firewall-Status**. Im Folgenden wird die Bedeutung der einzelnen Einstellungen erläutert:

- **Netzwerktyp** - Der Netzwerktyp, mit dem Ihr Computer verbunden ist.Endpoint Client verwendet grundlegende Firewall-Einstellung in Abhängigkeit von dem Netzwerktyp, mit dem Sie verbunden sind.

Netzwerktyp	Beschreibung
Vertrauensw.	Deaktiviert die Firewall für den entsprechenden Adapter.
Heim/Büro	Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk.
Öffentlich	Sämtlicher Datenverkehr wird gefiltert.
Unsicher	Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.

- **Stealth Modus** - Ob Sie von anderen Computern entdeckt werden können.

Status	Beschreibung
An	Stealth-Modus ist aktiviert.Ihr Computer ist sowohl im lokalen Netzwerk als auch im Internet unsichtbar.
Aus	Stealth-Modus ist deaktiviert.Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer entdecken.
Remote	Ihr Computer kann nicht im Internet entdeckt werden.Benutzer im lokalen Netzwerk können Ihren Computer entdecken

- **Gemeinsame Nutzung der Internetverbindung (ICS)** - Aktiviert die Unterstützung für die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing).

- **WLAN-Verbindungen überwachen** - Wenn Sie mit einem Drahtlosnetzwerk verbunden sind, werden Benachrichtigungen über bestimmte Netzwerkereignisse angezeigt (z.B. wenn ein neuer Computer mit dem Netzwerk verbunden wurde).

Privatsphärenschutz

Das Modul für den Privatsphärenschutz hilft Ihnen dabei, das wichtige persönliche Daten nicht in fremde Hände gelangen.Während Sie im Internet sind, schützt es Sie vor Phishing-Attacken, Betrugsversuchen, Missbrauch Ihrer privaten Daten und vielem mehr.

Dieses Modul hat zwei Funktionen:

- Phishing-Schutz: Macht das Surfen im Internet sicherer, indem es Phishing-Seiten und andere potenziell gefährliche Seiten blockiert und den Benutzer darauf hinweist.
- Datenschutz: Verhindert die unerlaubte Weitergabe sensibler Daten.

Für detaillierte Informationen zur Konfiguration des Privatsphärenschutzes, klicken Sie auf die Schaltfläche **Status des Privatsphärenschutzes**

Benutzerkontrolle

Endpoint Client enthält umfangreiche Benutzerkontrollen, um die Einhaltung von Richtlinien zur Computer- und Internet-Nutzung sicherzustellen.Ihr Netzwerkadministrator kann die folgenden Benutzerkontrollen konfigurieren:

- **Web-Kontrolle** - Filtert das Internetverhalten und setzt zeitliche Beschränkungen für den Internet-Zugriff fest.Über diese Steuerung kann der Administrator den Zugriff auf bestimmte Webseiten blockieren oder nur die Nutzung von Webseiten erlauben, die für die tägliche Aufgabenerfüllung benötigt werden.
- **Anwendungssteuerung** - Blockiert oder beschränkt den Zugriff auf bestimmte Anwendungen.
- **Schlüsselwortfilter** - Filtert den Zugriff auf Webseiten und E-Mail-Nachrichten anhand von Schlüsselwörtern.
- **Kategoriefilter** - blockiert festgelegte Kategorien von Web-Inhalten.So zum Beispiel soziale Netzwerke oder Filesharing-Seiten.

Um zu erfahren, welche Benutzerkontrollen für Sie festgelegt sind, klicken Sie auf **Status der Benutzerkontrolle**.

1.4. Surf-Schutz

Ihr Cloud Security for Endpoints-Administrator kann Sicherheitseinstellungen festlegen, die sich auf Ihre Internet-Nutzung auswirken können. Diese Sicherheitseinstellungen betreffen unter anderem:

- „Bitdefender-Symbolleiste“ (S. 7)
- „Suchberater“ (S. 7)

- „Gesperrte Webseiten“ (S. 7)

1.4.1. Bitdefender-Symbolleiste

Falls Ihr Cloud Security for Endpoints-Administrator dies eingerichtet hat, informiert Sie die Bitdefender-Symbolleiste über die Sicherheitsbewertung der von Ihnen aufgerufenen Webseite. Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten. Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird. Mit einem Klick auf den Dragger öffnen Sie die Symbolleiste.

Abhängig davon, wie Bitdefender die Webseite einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symbolleiste eingeblendet:

- Die Nachricht "Diese Website ist nicht sicher" erscheint auf rotem Hintergrund.
- Die Nachricht "Vorsicht ist geboten" erscheint auf orangefarbenem Hintergrund.
- Die Nachricht "Diese Website ist sicher" erscheint auf grünem Hintergrund.

1.4.2. Suchberater

Falls der Suchberater von Ihrem Cloud Security for Endpoints-Administrator eingerichtet wurde, bewertet dieser sowohl die Suchergebnisse von Google, Bing und Yahoo! als auch Links auf Facebook und Twitter, indem es ein Symbol vor jedem Ergebnis platziert. Im Folgenden finden Sie die verwendeten Symbole und deren Bedeutung:

Sie sollten diese Webseite nicht aufrufen.

Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen wollen.

Diese Seite ist sicher.

1.4.3. Gesperrte Webseiten

Abhängig von den von Ihrem Cloud Security for Endpoints-Administrator festgelegten Sicherheitsrichtlinien wurden unter Umständen bestimmte Surf-Schutz-Einstellungen eingerichtet, die Phishing-Angriffe und Internet-Betrugsversuche verhindern sollen. Cloud Security for Endpoints blockiert unter Umständen automatisch bekannte Phishing-Seiten (gefälschte Webseiten), um zu verhindern, dass Sie versehentlich private oder vertrauliche Informationen an Online-Betrüger weitergeben. Neben gefälschten Webseiten können auch andere Formen von Internet-Betrug unterdrückt werden, so zum Beispiel: Verkaufsbetrug, Get-Rich-Quick-Betrug, Internet-Marketing-Betrug, Klick-Betrug, usw. Anstelle der schädlichen Webseite wird eine spezielle Warnseite angezeigt, die Sie über die Gefahren der aufgerufenen Webseite informiert.

Beachten Sie
Falls Sie eine unbedenkliche Webseite aufrufen möchten, die fälschlicherweise erkannt und blockiert wurde, wenden Sie sich bitte an Ihren Cloud Security for Endpoints-Administrator, damit dieser die Seite freigeben kann.

1.5. Geräte-Scan

Endpoint Client kann konfiguriert werden automatisch Speichermedien (CDs/DVDs, USB Speicher oder Netzlaufwerke) zu entdecken und Sie auffordern diese zu Prüfen oder nicht.Im Warnfenster werden Informationen über das erkannte Gerät angezeigt.

Um das Gerät zu prüfen, clicken Sie **Ja**.Wenn Sie sicher sind, dass das Gerät sauber ist, können Sie wählen es nicht zu prüfen.

Beachten Sie
Falls mehrere Geräte gleichzeitig erkannt werden, wird für jedes Gerät nacheinander ein eigenes Warnfenster angezeigt.

Ihr Cloud Security for Endpoints-Administrator kann Endpoint Client-Warnungen und -Benachrichtigungen auch unterdrücken.In diesen Fällen wird der Geräte-Scan automatisch gestartet, ohne dass Sie sich darum kümmern müssen.

Wenn ein Geräte-Scan ausgeführt wird, wird ein entsprechendes Symbol für den Scan-Fortschritt in der Task-Leiste angezeigt.Doppelklicken Sie auf dieses Symbol, um das Scan-Fenster zu öffnen und den Scan-Fortschritt anzuzeigen.Sie können den Geräte-Scan jederzeit anhalten oder beenden.Weitere Informationen finden Sie unter „Antivirus Prüfassistent“ (S. 14).

1.6. Anpassen von Schutzeinstellungen

Die Konfiguration und Verwaltung von Endpoint Client erfolgt per Fernzugriff durch Ihren Netzwerkadministrator oder Dienstleister.Sie können die Schutzeinstellungen nicht bearbeiten.

Sollten Sie Fragen zu Ihren Schutzeinstellungen haben, wenden Sie sich bitte an den für Ihre Netzwerksicherheit verantwortlichen Mitarbeiter.

2. Prüfung auf Malware

Die Hauptaufgabe von Endpoint Client ist es, Ihren Computer frei von Schad-Software zu halten. Dies geschieht vornehmlich durch Echtzeit-Scans aller aufgerufenen Dateien, E-Mail-Nachrichen und aller neuen Dateien, die auf Ihren Computer heruntergeladen oder kopiert werden. Neben dem Echtzeitschutz ist auch möglich, Scans auszuführen, um Schad-Software auf Ihrem Computer zu erkennen und zu entfernen.

Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen.Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen.Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

2.1. Scannen von Dateien und Ordnern

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen.Rechtsklicken Sie auf die zu scannende Datei oder Verzeichnis und wählen Sie **Mit Bitdefender scannen**.Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

2.2. Ausführen eines Quick Scans

Beim Quick Scan wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Gehen Sie in den **Malware-Schutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Quick Scan** aus dem Dropdown-Menü.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen.Endpoint Client wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

2.3. Ausführen eines vollständigen System-Scans

Der vollständige System-Scan scannt den gesamten Computer nach allen Malware-Typen, die ein Sicherheitsrisiko darstellen, so zum Beispiel Viren, Spyware, Adware, Rootkits usw.

Beachten Sie
Da ein **Vollständiger System-Scan** einen gründlichen Scan des gesamten Systems durchführt, kann dieser einige Zeit in Anspruch nehmen. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.Für weitere Informationen lesen Sie bitte „Konfigurieren und Ausführen eines benutzerdefinierten Scans“ (S. 10).

Bevor Sie einen vollständigen System-Scan ausführen, sollten Sie Folgendes beachten:

- Stellen Sie sicher, dass die Malware-Signaturen von Endpoint Client immer auf dem neuesten Stand sind. Wenn Sie Ihren Computer auf Grundlage einer veralteten Signaturdatenbank scannen, könnte dies verhindern, dass Endpoint Client neue Malware erkennt, die seit dem letzten Update entdeckt wurde.Für weitere Informationen lesen Sie bitte „Updates“ (S. 18).
- Schließen Sie alle geöffneten Programme.

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Gehen Sie in den **Malware-Schutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Vollständigen System-Scan** aus dem Dropdown-Menü.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen.Endpoint Client wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans

Um einen Malware-Scan im Detail zu konfigurieren und dann auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Gehen Sie in den **Malware-Schutz**-Bereich.

3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Benutzerdefinierter Scan** aus dem Dropdown-Menü.
4. Bei Bedarf können einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste der **kürzlich durchgeführen Sans** bzw. der **Scan-Favoriten** klicken.
5. Klicken Sie auf **Ziel hinzufügen**, markieren Sie die Kästchen für die Bereiche, die Sie nach Malware durchsuchen wollen, und klicken Sie auf **OK**.
6. Klicken Sie auf **Scan-Optionen**, wenn Sie die Scan-Optionen konfigurieren wollen.Ein neues Fenster wird sich öffnen.Folgen Sie diesen Schritten:
   a. Sie können die Konfiguration einfach durch das Wählen der Scan-Tiefe festlegen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie den gewünschten Level erreicht haben.Nutzen Sie die Beschreibung auf der rechten Seite der Skala, um die Schutzstufe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

      Erfahrene Benutzer können die Scan-Einstellungen von Endpoint Client nutzen.Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Benutzerdefiniert**. Weitere Informationen zu den Optionen finden Sie am Ende dieses Kapitels.
   b. Sie können auch folgende allgemeine Optionen konfigurieren:
      - **Aufgabe mit niedriger Priorität ausführen .** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
      - **Scan-Assistent in die Task-Leiste minimieren .** Minimiert das Scan-Fenster in die Task-Leiste. Doppelklicken Sie auf das Symbol für den Scan-Fortschritt, um es wieder zu öffnen.
      - Wählen Sie die Aktion, die durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
   c. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.
7. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Assistenten für den Viren-Scan, um den Scan abzuschließen.Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen.Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Speichern eines benutzerdefinierten Scans in den Favoriten

Wenn Sie einen benutzerdefinierten Scan konfigurieren und ausführen, wird dieser automatisch zu einer begrenzten Liste von kürzlich durchgeführten Scans hinzugefügt.Wenn Sie einen benutzerdefinierten Scan später noch einmal verwenden möchten, können Sie ihn in der Liste der Scan-Favoriten unter einem eindeutigen Namen speichern.

Um einen kürzlich durchgeführten benutzerdefinierten Scan in der Liste der Scan-Favoriten zu speichern, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster für benutzerdefinierte Scans.
   a. Öffnen Sie das Endpoint Client-Fenster.
   b. Gehen Sie in den **Malware-Schutz**-Bereich.
   c. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Benutzerdefinierter Scan** aus dem Dropdown-Menü.
2. Durchsuchen Sie die Liste der **kürzlich durchgeführten Scans** nach dem gewünschten Scan.
3. Bewegen Sie den Mauszeiger auf den Namen des Scans und klicken Sie auf das Symbol ☆, um den Scan zur Liste der Scan-Favoriten hinzuzufügen.
4. Geben Sie einen eindeutigen Namen für den Scan ein.

Scans, die in den Favoriten gespeichert wurden, werden mit dem Symbol ★ gekennzeichnet.Wenn Sie auf dieses Symbol klicken, wird der Scan aus der Liste der Scan-Favoriten entfernt.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateitypen.** Sie können Endpoint Client so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden.Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.Diese Kategorie beinhaltet die folgenden Dateierweiterungen: `386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm;`

snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

Beachten Sie
Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Boot-Sektoren scannen.** Sie können Endpoint Client einstellen, damit die Boot-Sektoren gescannt werden.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Auf Rootkits prüfen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen.Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies prüfen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen.Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.

2.5. Antivirus Prüfassistent

Der Endpoint Client-Viren-Scan-Assistent erscheint, sobald Sie einen Bedarf-Scan starten (zum Beispiel indem Sie mit der rechten Maustaste auf einen Ordner klicken und dann **Mit Bitdefender scannen** auswählen).Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.

Beachten Sie

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen.Sehen Sie nach dem Prüffortschritticon im Systemtray.Doppelklicken Sie auf dieses Symbol, um das Scan-Fenster zu öffnen und den Scan-Fortschritt anzuzeigen.

2.5.1. Schritt 1 - Führen Sie den Scan durch

Endpoint Client startet den Scan der aus gewählten Dateien und Verzeichnisse.Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen).Klicken Sie auf **Mehr anzeigen**, um weitere Details zu erhalten.

Bitte warten Sie, bis der Scan abgeschlossen ist.Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

Stoppen oder pausieren der Prüfung. Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stopp** und **Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten.Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten.Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben.Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten, dass Endpoint Client Archive scannt, wählen Sie diese Option aus und geben das Passwort an.Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach einem Passwort fragen und dieses Objekt beim Scan überspringen.** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.
- **Alle Passwortgeschützte Datein überspringen ohne diese zu Prüfen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten.Endpoint Client kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

2.5.2. Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Beachten Sie

Wenn Sie einen Quick Scan oder einen vollständigen System-Scan durchführen, wird Endpoint Client während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind.Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen.Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Gewünschte Aktionen ausführen

Endpoint Client wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein.Endpoint Client wird automatisch versuchen, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren.Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

  Wichtig

  Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Endpoint Client versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann.Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Löschen

Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Endpoint Client versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren.Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Keine Aktion durchführen

Es wird keine Aktion für die infizierte Dateien ausgeführt.Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

2.5.3. Schritt 3 - Zusammenfassung

Wenn Endpoint Client die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt.Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **Logdatei anzeigen**.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

Wichtig

In den meisten Fällen desinfiziert Endpoint Client erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion.Dennoch gibt es Probleme, die nicht automatisch gelöst werden können.Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

2.6. Scan-Protokolle werden überprüft

Für jeden Scan wird ein Protokoll erstellt.Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Um die Scan-Protokolle zu einem späteren Zeitpunkt zu überprüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Klicken Sie auf **Malware-Schutz** im Menü auf der linken Seite.Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
4. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden.Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.Die Berichtdatei wird in Ihrem Webbrowser geöffnet.

3. Updates

In einer Welt, in der Internet-Kriminelle immer neue Wege finden, um Ihnen zu schaden, ist es von größter Wichtigkeit, dass Sie Ihre Sicherheitslösung zu jeder Zeit auf dem neuesten Stand halten, um stets einen Schritt voraus zu sein.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung mit dem Internet verbunden sind, arbeitet die Endpoint Client-Software eigenständig. Sie überprüft zunächst beim Start des Computers und danach **stündlich**, ob neue Updates verfügbar sind.Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Beachten Sie

Die standardmäßige Frequenz für automatische Updates kann von Ihrem Netzwerkadministrator angepasst werden.Für weitere Informationen lesen Sie bitte „Wobei handelt es sich bei der Frequenz für automatische Updates?“ (S. 20).

Der Update-Vorgang wird "on-the-fly" durchgeführt. Das bedeutet, dass die Dateien, die aktualisiert werden sollen, nach und nach ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen.Für weitere Informationen lesen Sie bitte „Durchführung eines Updates“ (S. 19).

3.1. Arten von Updates

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates der Malware-Signaturen** - Immer wenn neue Bedrohungen auftreten, müssen die Dateien mit den Malware-Signaturen aktualisiert werden, um einen durchgängigen und aktuellen Schutz zu gewährleisten.
- **Produkt-Updates** - wenn eine neue Version auf dem Markt erscheint, enthält diese zur Leistungssteigerung des Produkts neue Funktionen und Scantechniken.

  Bei einem Produkt-Upgrade handelt es sich um eine neue Hauptversion der Software.

3.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist

Um zu überprüfen, ob Ihr Schutz auf dem neuesten Stand ist, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Update**.
3. Der Update-Status und der Zeitpunkt der letzten Update-Überprüfung und Update-Installation werden angezeigt.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Klicken Sie im Hauptfenster in der oberen Symbolleiste auf **Ereignisse**.
2. Klicken Sie im Menü links auf **Update**.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen).Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

3.3. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Sie haben folgende Möglichkeiten, ein Update zu starten:

- Öffnen Sie das Endpoint Client-Fenster, klicken Sie in der oberen Symbolleiste auf die **Update**-Schaltfläche und wählen Sie dann **Update**.
- Rechtsklicken Sie in der Task-Leiste auf das Bitdefender-Symbol und wählen Sie **Update jetzt durchführen**.

Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates.Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Wichtig
Möglicherweise kann ein Neustart nach Abschluss des Updates notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst zeitnah durchzuführen.

3.4. Wobei handelt es sich bei der Frequenz für automatische Updates?

Um die Frequenz der automatischen Updates anzuzeigen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Update**.
3. Im Feld **Automatisches Update** können Sie überprüfen, wie oft automatische Updates ausgeführt werden.

4. Ereignisse

Endpoint Client führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich der Computer-Aktivitäten, die von der Benutzerkontrolle überwacht werden).Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung Ihres Bitdefender-Schutzes.So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.

Um das Ereignisprotokoll aufzurufen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Client-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Wählen Sie im Menü links die Ereigniskategorie aus.Ereignisse sind in die folgenden Kategorien unterteilt:
   - **Malware-Schutz**
   - **Firewall**
   - **Privatsphärenschutz**
   - **Benutzerkontrolle**
   - **Update**
   - **Verschiedenes**

   Über jedem Kategorienamen wird auf rotem Hintergrund die Anzahl der ungelesenen kritischen Ereignisse oder Fehlermeldungen angezeigt.

Eine Liste von Ereignissen ist für jede Kategorie verfügbar.Um weitere Informationen über ein bestimmtes Ereignis in der Liste zu erhalten, müssen Sie nur darauf klicken. Details zu dem Ereignis werden in der unteren Hälfte des Fensters angezeigt.Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender für beim Auftreten des Ereignisses durchgeführt hat; das Datum und der Zeitpunkt des Ereignisses.

Sie können Ereignisse nach Ihrer Dringlichkeit ordnen.Es gibt drei Arten von Ereignissen. Diese werden durch verschiedene Symbole unterschieden:

Information Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.
Warnung Diese Ereignisse weisen auf nicht-kritische Probleme hin.
Kritische Ereignisse weisen auf kritische Probleme hin.

Um Ihnen die Verwaltung von protokollierten Ereignissen zu erleichtern, enthält jeder Abschnitt des Ereignisfensters Optionen, mit denen Sie alle Ereignisse in diesem Abschnitt filtern oder als gelesen markieren können.Ereignisse können nur von Ihrem Netzwerkadministrator gelöscht werden.

5. Hilfe erhalten

Sollten Sie Probleme oder Fragen zu Endpoint Client, wenden Sie sich bitte an Ihren Netzwerkadministrator oder Dienstleister.

Um Produkt- und Kontaktinformationen zu finden, können Sie folgendermaßen vorgehen:

- Öffnen Sie das Endpoint Client-Fenster und klicken Sie in der unteren rechten Bildschirmecke auf das **Info**-Symbol.
- Rechtsklicken Sie in der Task-Leiste auf das Bitdefender-Symbol und wählen Sie **Über**.

Glossar

Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

AktiveX

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann.Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden.Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen.AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Arbeitsspeicher

Interne Speicherzonen im Rechner.Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips.Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet.Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Autostart-Einträge

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können

Autostart-Objekte sein.Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette.Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert.Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert.Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS.Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte.Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät.Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner.Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

Durchsuchen

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird.Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer.Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

E-Mail Client

Ein E-Mail-Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Ereignisse

Ereignisse oder Erscheinungen, die in einem Programm vorkommen.Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Heuristik

Eine Methode, um neue Viren zu identifizieren.Diese Prüfmethode beruht nicht auf spezifische Virussignaturen.Der Vorteil einer heuristischen Prüfung ist, dass man nicht

von einer neuen Virusvariante getäuscht werden kann.Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft.Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an.Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus.Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben.Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind nicht grundsätzlich als schädlich anzusehen. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen vorsätzlich als kriminelles Mittel eingesetzt (um beispielsweise private Daten wie Anmeldedaten oder Kreditkartendaten zu sammeln).

Komprimierte Programme

Eine Datei in einem komprimierten Format.Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt.Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält.Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden.In diesem Fall sind nur noch zwei Bytes notwendig statt zehn.Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Logdatei mit den gescannten Pfaden, Verzeichnissen und der Archivanzahl sowie den gescannten, infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird.Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bösartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Signatur

Malware-Signaturen sind Code-Bruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet.Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.
Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur.Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet.Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail weist den Empfänger an, eine Webseite zu besuchen, auf der dieser bestimmte persönlichen Daten aktualisieren soll, so z.B. Passwörter oder Kreditkarten- und Kontonummern, die dem tatsächlichen Unternehmen bereits mitgeteilt wurden. Bei der Website handelt es sich allerdings um eine Fälschung, die einzig und allein zum Zwecke des Informationsdiebstahls erstellt wurde.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert.Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Port

Stelle eines Computers, an die ein Gerät angeschlossen werden kann. Computer haben verschiedene Arten solcher Schnittstellen. Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen.Die Schnittstellennummer gibt die Art der Schnittstelle an.Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Software-Tools die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

Skript

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Beiträge in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer Anwenderdaten über seine Internetverbindung sammelt. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an Dritte. Spyware kann auch Informationen über E-Mail-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren.Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden.Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden.TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt.Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein.Einer der heimtückischsten Trojaner

ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das manuelle oderautomatische Scans nach Updates ermöglicht.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt.Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein.Die meisten Viren können sich selber vervielfältigen.Alle Computerviren sind von Menschenhand geschrieben.Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben.Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Wurm

Ein Programm, das sich über ein Netzwerk verbreitet.Es kann sich nicht an andere Programme anhängen.